

# IP Address Affinity

Findings from an Internet Society Roundtable  
May 2009

## ***Background***

Technologists are discussing a number of shared addressing schemes for use when IPv4 addresses become harder to obtain and more addresses are still needed. All of the approaches proposed to address this situation include a transition from the approach today in which a single household generally is assigned a single public IPv4 address that is shared among devices in the household, to a situation where a single public IPv4 address is shared across a potentially large number of households.<sup>1</sup> This has included a discussion of shared addresses in the Internet Engineering Task Force (IETF).<sup>2</sup>

As part of its efforts to foster discussion of issues affecting the ongoing evolution of the Internet, the Internet Society organized a roundtable in May of 2009 and invited both network operators and content providers. Discussion focused on assumptions being made by application developers and content providers about the network, and specifically on how the adoption of shared addressing solutions by operators might impact the assumptions and service offerings of content providers. Based on discussions at the Internet Society roundtable, this paper documents some aspects of how content and service providers use IP addresses today, and some of the implications for service providers, content providers, and end users during a transition period in which the current assumptions about IP addresses no longer hold.

## ***Assumptions about IP Addresses Made in the Internet today***

After discussing the different approaches to sharing IP addresses in IPv4 and some of the operations this might break, roundtable participants agreed to make a list of things that are assumed about network operations in a scenario where a single IPv4 address is assigned to an end user household, and how changing that assumption would break existing functionality in the network. The important point is that today business models and commercial contracts are based on these assumptions and those business models and commercial contracts may not be sustainable as these assumptions change. Furthermore, because these assumptions are not explicit, it is possible that these changes will be made without all affected parties realizing the full impact of them in advance.

Such an observation underlines the importance of preserving (restoring) end-to-end connectivity in the Internet. A solution for this is the ultimate transition to IPv6 where address sharing is not necessary.

---

<sup>1</sup> See references at the end of this report for documents describing the issue of IPv4 address exhaustion and various proposed approaches.

<sup>2</sup> See <http://www.ietf.org/internet-drafts/draft-ford-shared-addressing-issues-01.txt> for the Internet Draft and <http://www.ietf.org/proceedings/74/minutes/shara.txt> for minutes of the meeting at IETF 74.

The group identified the following uses of IPv4 in services today, all of which make some assumptions about what an IPv4 address tells a service or content provider about their users:

1. **Geolocation:** an IP address tells one with some level of granularity and some level of confidence where a host is physically located. Content providers build services on this such as content licensing and content restriction, ad targeting, and emergency services. For example, someone may have a license to stream content to a particular geographical area but not to another and the IP address is used to determine the location of the receiving host (with some level of statistical confidence). Transition to a model where new end-users are connected to the Internet through some sort of carrier grade NAT device<sup>3</sup> that is not geographically near the end-user destroys the confidence in the location of the end-user and thus disrupts the service offering built on today's assumption.
2. **Geoproximity:** a slightly different use of an IP address is based on the proximity of a host to a particular service delivery point. This in particular impacts the efficient delivery of content to an end-user. For example, if a carrier-grade NAT is introduced in communications and it is far from an end-user connected to it, there will likely be some performance degradation for services that depend on geoproximity to ensure efficient delivery of content.
3. **Identifying abusers:** today an abuser of a network or network service is associated with an IP address. When such abuse is detected any traffic from the associated IP address may be blocked from further disrupting the service. This works fairly well when an IP address identifies a single household, but in cases where the IP address is shared across a large number of households, a large number of unrelated end-users may be blocked from a service when in fact only one of them is responsible for abusing the service. In cases today where a large number of users are behind a NAT in an enterprise, the enterprise has methods for detecting and stopping the abuser once someone else from the enterprise complains about being blocked from a service. When multiple users behind a NAT in a residential situation complain of having access to a service blocked it is unclear exactly how the situation will be resolved, but it will probably go through the provider of the residential service which increases cost for them as well as for any end service provider who is impacted. An example of these kind of effects can be seen in the incident where Wikipedia blocked everyone in Qatar from access due to the fact that the whole country shares a single IP address (<http://news.bbc.co.uk/2/hi/technology/6224677.stm>).
4. **Spam:** another case of identifying abusers has to do with spam blacklisting. When a spammer is behind a carrier-grade NAT or using a port-shared address, blacklisting of their IP will result in all other subscribers sharing that address having their ability to source SMTP packets restricted to some

---

<sup>3</sup> A device that resides in a network allowing the sharing of a single public address across many households or many end-user devices.

extent. It is unclear where the cost for this lands, but it is likely again that service providers will have a negative impact to their business from dealing with unhappy customers.

5. **Authentication and security:** Simple address based identification mechanisms that are used to shape access control lists (ACLs) will break when the IP address is no longer sufficient to identify a particular subscriber for example. To add address and port number combinations increases the complexity of the ACL itself, and may require making the port number assignments more static than service providers would like or some complicated infrastructure to update ACLs dynamically.
6. **Lawful intercept/forensics:** IP addresses and their use intervals are logged in various ways by providers of end-user services today. As address sharing is introduced, these logs will have to include at least port assignments as well as addresses. The participants in the roundtable meeting observed that whereas today it is sufficient to log activity based on IP addresses, in the future it will be necessary to also log source ports. While source port logging can help with identifying abusers, it requires much greater storage resources for the expanded logging information and searching that information in response to law enforcement queries more challenging.

The following table briefly summarizes the use of the address, the impacted service, and who feels this impact.

**TABLE 1: Summary of IP Address Affinity**

| Capability                  | Impacted Service                             | Affected  |
|-----------------------------|--|---|
| Geolocation                 | Any that uses                                | Access providers, content providers, and end-users  |
| Geoproximity                | Content distribution                         | End-user (response), Internet (inefficient routing of information), content providers (difficulty in delivering a responsive service) |
| Identifying service abusers | All  | Operator of the service, end-users  |
| Spam                        | Blacklisting IP addresses                    | End-users, access providers, operator of the blacklisting service   |
| Authentication and Security | Any service employing IP address-based ACLs  | Access provider, service provider   |
| Lawful Intercept            | Address logging (will need to add ports now) | Access provider   |
|                             |  |   |

## ***Participants***

The following people participated in the ISOC Spring 2009 Operator and Service Provider Summit and contributed to this discussion of the relevant issues:

Lorenzo Colliti (Google), Erik Kline (Google), Igor Gashinsky (Yahoo), Jason Fesler (Yahoo), Rick Reed (Yahoo), Adam Bechtel (Yahoo), Larry Campbell (Akamai), Tom Coffeen (Limelight), David Temkin (Netflix), John Brzozowski (Comcast), Alain Durand (Comcast), Pete Gelbman (Clearwire), Mark Winter (Clearwire), Will Charnock (The Planet), Martin Levy (Hurricane Electric), Leslie Daigle (ISOC), Mat Ford (ISOC), Phil Roberts (ISOC), Greg Wood (ISOC).

## ***References***

1. Durand, A., ed., "Dual-stack lite broadband deployments post IPv4 exhaustion," draft-ietf-softwire-dual-stack-lite-01 (work in progress), July 2009.
2. Nishitani, T., Miyakawa, S., Nakagawa, A., and H. Ashida, "Common Functions of Large Scale NAT (LSN)," draft-nishitani-cgn-02 (work in progress), June 2009.
3. Boucadair, M., Levis, P., Bajko, G., and T. Savolainen, "IPv4 Connectivity Access in the Context of IPv4 Address Exhaustion: Port Range based IP Architecture," draft-boucadair-port-range-02 (work in progress), July 2009.
4. Shirasaki, Y., Miyakawa, S., Nakagawa, A., Yamaguchi, J., and H. Ashida, "ISP Shared Address," draft-shirasaki-isp-shared-addr-02 (work in progress), March 2009.
5. Bush, R., "The A+P Approach to the IPv4 Address Shortage," draft-ymbk-aplusp-04 (work in progress), July 2009.

## ***About the Internet Society***

The Internet Society is a non-profit organization founded in 1992 to provide leadership in Internet related standards, education, and policy. With offices in Washington, D.C., and Geneva, Switzerland, it is dedicated to ensuring the open development, evolution, and use of the Internet for the benefit of people throughout the world. More information is available at: <http://InternetSociety.org>